

1 **In the Claims**

2 Claims 1, 7, 13, 18, 22 and 26 are amended.

3 Claims 1-31 remain in the application and are listed below:

4
5 1. **(CURRENTLY AMENDED)** A Web server input string screening
6 method comprising:

7 determining an attack pattern that can be used to attack a Web server, the
8 attack pattern comprising content that is designed to constitute one or more of a
9 disclosure attack, an integrity attack or a denial of service attack on the Web
10 server;

11 defining a search pattern that can be used to detect the attack pattern, the
12 search pattern being defined in a manner that permits variability among its
13 constituent parts;

14 receiving an input string that is intended for use by a Web server;

15 evaluating the input string using the search pattern to ascertain whether the
16 attack pattern is present; and

17 implementing a remedial action if an attack pattern is found that matches
18 the search pattern.

19
20 2. **(ORIGINAL)** The Web server input string screening method of
21 claim 1, wherein:

22 said defining comprises defining a plurality of different search patterns; and

23 said evaluating comprises evaluating the input string using said plurality of
24 different search patterns.

1 3. **(ORIGINAL)** The Web server input string screening method of
2 claim 1, wherein the search pattern is specified as a regular expression.

3
4 4. **(ORIGINAL)** The Web server input string screening method of
5 claim 1, wherein said receiving of the input string comprises receiving a URL.

6
7 5. **(ORIGINAL)** The Web server input string screening method of
8 claim 1, wherein said receiving of the input string comprises receiving a portion of
9 an HTTP verb request.

10
11 6. **(ORIGINAL)** The Web server input string screening method of
12 claim 1, wherein said implementing comprises denying a request that is associated
13 with the input string.

14
15 7. **(CURRENTLY AMENDED)** A Web server input string screening
16 method comprising:

17 defining one or more search patterns that comprise literal characters and
18 special characters, wherein the literal characters indicate exact characters in an
19 input string that is intended for receipt by a Web server, and the special characters
20 indicate variable characters in an input string that is intended for receipt by the
21 Web server, the search patterns being usable to search for an attack pattern that
22 can be used to attack the Web server, the attack pattern comprising content that is
23 designed to constitute one or more of a disclosure attack, an integrity attack or a
24 denial of service attack on the Web server; and
25

1 storing the one or more search patterns in a memory location that is
2 accessible to a screening tool for evaluating an input string that is intended for
3 receipt by the Web server.

4
5 8. **(ORIGINAL)** The Web server input string screening method of
6 claim 7 further comprising:

7 retrieving a search pattern from the memory location; and

8 evaluating an input string with the screening tool by ascertaining whether
9 the input string includes at least a portion that matches the search pattern.

10
11 9. **(ORIGINAL)** The Web server input string screening method of
12 claim 8, wherein the evaluating of the input string comprises evaluating a URL.

13
14 10. **(ORIGINAL)** The Web server input string screening method of
15 claim 8, wherein the evaluating of the input string comprises evaluating a portion
16 of an HTTP verb request.

17
18 11. **(ORIGINAL)** The Web server input string screening method of
19 claim 7 further comprising implementing the screening tool as an extension for an
20 existing Web server.

21
22 12. **(ORIGINAL)** The Web server input string screening method of
23 claim 7 further comprising implementing the screening tool as an ISAPI extension.

1 13. (CURRENTLY AMENDED) A Web server input string screening
2 method comprising:

3 defining one or more search patterns that are specified as a regular
4 expression, the search patterns being usable to search for an attack pattern that can
5 be used to attack the Web server, the attack pattern comprising content that is
6 designed to constitute one or more of a disclosure attack, an integrity attack or a
7 denial of service attack on the Web server; and

8 storing the one or more search patterns in a memory location that is
9 accessible to a screening tool for evaluating an input string that is intended for
10 receipt by the Web server.

11
12 14. (ORIGINAL) The Web server input string screening method of
13 claim 13 further comprising:

14 retrieving a search pattern from the memory location; and

15 evaluating an input string with the screening tool by ascertaining whether
16 the input string includes at least a portion that matches the search pattern.

17
18 15. (ORIGINAL) The Web server input string screening method of
19 claim 14, wherein the evaluating of the input string comprises evaluating a URL.

20
21 16. (ORIGINAL) The Web server input string screening method of
22 claim 14, wherein the evaluating of the input string comprises evaluating a portion
23 of an HTTP verb request.
24
25

1 17. (ORIGINAL) A computer-readable medium having computer-
2 readable instructions thereon which, when executed by a computer, perform the
3 method of claim 14.

4
5 18. (CURRENTLY AMENDED) A Web server input string screening
6 tool embodied on a computer-readable medium comprising:

7 a pattern matching engine that is configured to receive an input string that
8 is intended for use by a Web server and evaluate the input string to ascertain
9 whether it likely constitutes an attack on the Web server, the attack comprising
10 one or more of a disclosure attack, an integrity attack or a denial of service attack
11 on the Web server; and

12 one or more patterns that are usable by the pattern matching engine to
13 evaluate the input string, the patterns being defined in a manner that permits
14 variability among the constituent parts of the one or more patterns.

15
16 19. (ORIGINAL) The Web server input string screening tool of claim
17 18, wherein the one or more patterns are specified as regular expressions.

18
19 20. (ORIGINAL) The Web server input string screening tool of claim
20 18, wherein the pattern matching engine is configured to receive an input string
21 that comprises a URL.

22
23 21. (ORIGINAL) The Web server input string screening tool of claim
24 18, wherein the pattern matching engine is configured to receive an input string
25 that comprises a portion of an HTTP verb request.

1
2 22. **(CURRENTLY AMENDED)** One or more computer readable
3 media having computer-readable instructions thereon which, when executed by a
4 computer perform the following steps:

5 receiving an input string that is intended for use by a Web server;

6 evaluating the input string using a search pattern to ascertain whether the
7 input string contains an attack pattern that can be used to attack the Web server,
8 the attack pattern comprising content that is designed to constitute one or more of
9 a disclosure attack, an integrity attack or a denial of service attack on the Web
10 server, the search pattern comprising literal characters and special characters,
11 wherein literal characters indicate exact characters in the input string, and the
12 special characters indicate variable characters in the input string; and

13 implementing a remedial action if an attack pattern is found that matches
14 the search pattern.

15
16 23. **(ORIGINAL)** The computer-readable media of claim 22, wherein
17 said implementing comprises denying a request that is associated with the input
18 string.

19
20 24. **(ORIGINAL)** The computer-readable media of claim 22, wherein
21 said receiving comprises receiving a URL.
22
23
24
25

1 25. **(ORIGINAL)** The computer-readable media of claim 22, wherein
2 said receiving comprises receiving an input string that is associated with an HTTP
3 verb request.

4
5 26. **(CURRENTLY AMENDED)** A collection of Web server screening
6 patterns embodied on a computer-readable medium comprising:

7 a memory; and

8 a plurality of ~~attack~~ patterns stored in the memory, the ~~attack~~ patterns being
9 useable to screen input strings that are intended for use by a Web server to
10 ascertain whether the input strings comprise attack patterns, the attack patterns
11 comprising content that is designed to constitute one or more of a disclosure
12 attack, an integrity attack or a denial of service attack on the Web server,
13 individual ~~attack~~ patterns being defined in a manner that permits variability among
14 their constituent parts.

15
16 27. **(ORIGINAL)** The collection of claim 26, wherein the patterns are
17 specified as regular expressions.

18
19 28. **(ORIGINAL)** The collection of claim 26, wherein the collection is
20 adapted for addition to, deletion of, or modification of patterns.

21
22 29. **(ORIGINAL)** The collection of claim 26, wherein the patterns are
23 configured for use in screening URLs that are intended for use by a Web server.

30. (ORIGINAL) The collection of claim 26, wherein the patterns are configured for use in screening input strings associated with HTTP verb requests that are intended for use by a Web server.

31. (ORIGINAL) The collection of claim 26 configured for use by an ISAPI extension.